



Date de réception : 23/01/2015



Published ID	: C-362/14
Document number	: 13
Register number	: 976996
Date of lodgment	: 03/11/2014
Date of entry in the register	: 03/11/2014
Type of document	: Observations
Lodgment reference	: Annexes Part 3
File number	: DC33346
Person lodging document	: Julie Vondung (R249125) Commission

Annex 3

Communication from the Commission to the European Parliament and the Council, "Rebuilding Trust in EU-US Data Flows", COM(2013) 846, 27.11.2013, referred to in paragraphs 29 and 30 of the observations.



Brussels, 27.11.2013
COM(2013) 846 final

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT AND THE COUNCIL**

Rebuilding Trust in EU-US Data Flows

1. INTRODUCTION: THE CHANGING ENVIRONMENT OF EU-US DATA PROCESSING

The European Union and the United States are strategic partners, and this partnership is critical for the promotion of our shared values, our security and our common leadership in global affairs.

However, trust in the partnership has been negatively affected and needs to be restored. The EU, its Member States and European citizens have expressed deep concerns at revelations of large-scale US intelligence collection programmes, in particular as regards the protection of personal data¹. Mass surveillance of private communication, be it of citizens, enterprises or political leaders, is unacceptable.

Transfers of personal data are an important and necessary element of the transatlantic relationship. They form an integral part of commercial exchanges across the Atlantic including for new growing digital businesses, such as social media or cloud computing, with large amounts of data going from the EU to the US. They also constitute a crucial component of EU-US co-operation in the law enforcement field, and of the cooperation between Member States and the US in the field of national security. In order to facilitate data flows, while ensuring a high level of data protection as required under EU law, the US and the EU have put in place a series of agreements and arrangements.

Commercial exchanges are addressed by Decision 2000/520/EC² (hereafter “the Safe Harbour Decision”). This Decision provides a legal basis for transfers of personal data from the EU to companies established in the US which have adhered to the Safe Harbour Privacy Principles.

Exchange of personal data between the EU and the US for the purposes of law enforcement, including the prevention and combating of terrorism and other forms of serious crime, is governed by a number of agreements at EU level. These are the Mutual Legal Assistance Agreement³, the Agreement on the use and transfer of Passenger Name Records (PNR)⁴, the Agreement on the processing and transfer of Financial Messaging Data for the purpose of the Terrorist Finance Tracking Program (TFTP)⁵, and the Agreement between Europol and the US. These Agreements respond to important security challenges and meet the common security interests of the EU and US, whilst providing a high level of protection of personal data. In addition, the EU and the US are currently negotiating a framework agreement on data protection in the field of police and judicial cooperation (“umbrella agreement”)⁶. The aim is to ensure a high level of data protection for citizens whose data is exchanged thereby further

¹ For the purposes of this Communication, references to EU citizens include also non-EU data subjects which fall within the scope of European Union's data protection law.

² Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, p. 7.

³ Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 291, 7.11.2009, p. 40.

⁴ Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L215, 11.8.2012, p. 4.

⁵ Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.7.2010, p. 3.

⁶ The Council adopted the Decision authorising the Commission to negotiating the Agreement on 3 December 2010. See IP/10/1661 of 3 December 2010.

advancing EU-US cooperation in the combating of crime and terrorism on the basis of shared values and agreed safeguards.

These instruments operate in an environment in which personal data flows are acquiring increasing relevance.

On the one hand, the development of the digital economy has led to exponential growth in the quantity, quality, diversity and nature of data processing activities. The use of electronic communication services by citizens in their daily lives has increased. Personal data has become a highly valuable asset: the estimated value of EU citizens' data was €315bn in 2011 and has the potential to grow to nearly €1tn annually by 2020⁷. The market for the analysis of large sets of data is growing by 40% per year worldwide⁸. Similarly, technological developments, for example related to cloud computing, put into perspective the notion of international data transfer as cross-border data flows are becoming a day to day reality.⁹

The increase in the use of electronic communications and data processing services, including cloud computing, has also substantially expanded the scope and significance of transatlantic data transfers. Elements such as the central position of US companies in the digital economy¹⁰, the transatlantic routing of a large part of electronic communications and the volume of electronic data flows between the EU and the US have become even more relevant.

On the other hand, modern methods of personal data processing raise new and important questions. This applies both to new means of large-scale processing of consumer data by private companies for commercial purposes, and to the increased ability of large-scale surveillance of communications data by intelligence agencies.

Large-scale US intelligence collection programmes, such as PRISM affect the fundamental rights of Europeans and, specifically, their right to privacy and to the protection of personal data. These programmes also point to a connection between Government surveillance and the processing of data by private companies, notably by US internet companies. As a result, they may therefore have an economic impact. If citizens are concerned about the large-scale processing of their personal data by private companies or by the surveillance of their data by intelligence agencies when using Internet services, this may affect their trust in the digital economy, with potential negative consequences on growth.

These developments expose EU-US data flows to new challenges. This Communication addresses these challenges. It explores the way forward on the basis of the findings contained in the Report of the EU Co-Chairs of the ad hoc EU-US Working Group and the Communication on the Safe Harbour.

It seeks to provide an effective way forward to rebuild trust and reinforce EU-US cooperation in these fields and strengthen the broader transatlantic relationship.

This Communication is based on the premise that the standard of protection of personal data must be addressed in its proper context, without affecting other dimensions of EU-US relations, including the on-going negotiations for a Transatlantic Trade and Investment Partnership. For this reason, data protection standards will not be negotiated within the Transatlantic Trade and Investment Partnership, which will fully respect the data protection rules.

⁷ See Boston Consulting Group, "The Value of our Digital Identity", November 2012.

⁸ See McKinsey, "Big data: The next frontier for innovation, competition, and productivity", 2011

⁹ Communication on Unleashing the potential of cloud computing in Europe, COM(2012) 529 final

¹⁰ For example, the combined number of unique visitors to Microsoft Hotmail, Google Gmail and Yahoo! Mail from European countries in June 2012 totalled over 227 million, eclipsing that of all other providers. The combined number of unique European users accessing Facebook and Facebook Mobile in March 2012 was 196.5 million, making Facebook the largest social network in Europe. Google is the leading internet search engine with 90.2% of worldwide internet users. US mobile messaging service What's App was used by 91% of iPhone users in Germany in June 2013.

It is important to note that whilst the EU can take action in areas of EU competence, in particular to safeguard the application of EU law¹¹, national security remains the sole responsibility of each Member State¹².

2. THE IMPACT ON THE INSTRUMENTS FOR DATA TRANSFERS

First, as regards data transferred for commercial purposes, the Safe Harbour has proven to be an important vehicle for EU-US data transfers. Its commercial importance has grown as personal data flows have taken on greater prominence in the transatlantic commercial relationship. Over the past 13 years, the Safe Harbour scheme has evolved to include more than 3.000 companies, over half of which have signed up within the last five years. Yet concerns about the level of protection of personal data of EU citizens transferred to the US under the Safe Harbour scheme have grown. The voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement. While a majority of US companies apply its principles, some self-certified companies do not. The non-compliance of some self-certified companies with the Safe Harbour Privacy Principles places such companies at a competitive advantage in relation to European companies operating in the same markets.

Moreover, while under the Safe Harbour, limitations to data protection rules are permitted where necessary on grounds of national security¹³, the question has arisen whether the large-scale collection and processing of personal information under US surveillance programmes is necessary and proportionate to meet the interests of national security. It is also clear from the findings of the ad hoc EU-US Working Group that, under these programmes, EU citizens do not enjoy the same rights and procedural safeguards as Americans.

The reach of these surveillance programmes, combined with the unequal treatment of EU citizens, brings into question the level of protection afforded by the Safe Harbour arrangement. The personal data of EU citizens sent to the US under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the EU and the purposes for which it was transferred to the US. A majority of the US internet companies that appear to be more directly concerned by these programmes are certified under the Safe Harbour scheme.

Second, as regards exchanges of data for law enforcement purposes, the existing Agreements (PNR, TFTP) have proven highly valuable tools to address common security threats linked to serious transnational crime and terrorism, whilst laying down safeguards that ensure a high level of data protection¹⁴. These safeguards extend to EU citizens, and the Agreements provide for mechanisms to review their implementation and to address issues of concern related thereto. The TFTP Agreement also establishes a system of oversight, with EU independent overseers checking how data covered by the Agreement is searched by the US.

Against the backdrop of concerns raised in the EU about US surveillance programmes, the European Commission has used those mechanisms to check how the agreements are applied. In the case of the PNR Agreement, a joint review was conducted, involving data protection

¹¹ See Judgment of the Court of Justice of the European Union in Case C-300/11, ZZ v Secretary of State for the Home Department.

¹² Article 4(2) TEU.

¹³ See e.g. Safe Harbour Decision, Annex I.

¹⁴ See Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.

experts from the EU and the US, looking at how the Agreement has been implemented¹⁵. That review did not give any indication that US surveillance programmes extend to or have impact on the passenger data covered by the PNR Agreement. In the case of the TFTP Agreement, the Commission opened formal consultations after allegations were made of US intelligence agencies directly accessing personal data in the EU, contrary to the Agreement. These consultations did not reveal any elements proving a breach of the TFTP Agreement, and they led the US to provide written assurance that no direct data collection has taken place contrary to the provisions of the Agreement.

The large-scale collection and processing of personal information under US surveillance programmes call, however, for a continuation of very close monitoring of the implementation of the PNR and TFTP Agreements in the future. The EU and the US have therefore agreed to advance the next Joint Review of the TFTP Agreement, which will be held in Spring 2014. Within that and future joint reviews, greater transparency will be ensured on how the system of oversight operates and on how it protects the data of EU citizens. In parallel, steps will be taken to ensure that the system of oversight continues to pay close attention to how data transferred to the US under the Agreement is processed, with a focus on how such data is shared between US authorities.

Third, the increase in the volume of processing of personal data underlines the importance of the legal and administrative safeguards that apply. One of the goals of the Ad Hoc EU-US Working Group was to establish what safeguards apply to minimise the impact of the processing on the fundamental rights of EU citizens. Safeguards are also necessary to protect companies. Certain US laws such as the Patriot Act, enable US authorities to directly request companies access to data stored in the EU. Therefore, European companies, and US companies present in the EU, may be required to transfer data to the US in breach of EU and Member States' laws, and are consequently caught between conflicting legal obligations. Legal uncertainty deriving from such direct requests may hold back the development of new digital services, such as cloud computing, which can provide efficient, lower-cost solutions for individuals and businesses.

3. ENSURING THE EFFECTIVENESS OF DATA PROTECTION

Transfers of personal data between the EU and the US are an essential component of the transatlantic commercial relationship. Information sharing is also an essential component of EU-US security cooperation, critically important to the common goal of preventing and combating serious crime and terrorism. However, recent revelations about US intelligence collection programmes have negatively affected the trust on which this cooperation is based. In particular, it has affected trust in the way personal data is processed. The following steps should be taken to restore trust in data transfers for the benefit of the digital economy, security both in the EU and in the US, and the broader transatlantic relationship.

3.1. The EU data protection reform

The data protection reform proposed by the Commission in January 2012¹⁶ provides a key response as regards the protection of personal data. Five components of the proposed Data Protection package are of particular importance.

¹⁵ See on the Commission report "Joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security".

¹⁶ COM(2012) 10 final: Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.1.2012, and COM(2012) 11 final: Proposal for a Regulation of the European Parliament and the Council on the protection of individuals

First, as regards territorial scope, the proposed regulation makes clear that companies that are not established in the Union will have to apply EU data protection law when they offer goods and services to European consumers or monitor their behaviour. In other words, the fundamental right to data protection will be respected, independently of the geographical location of a company or of its processing facility¹⁷.

Secondly, on international transfers, the proposed regulation establishes the conditions under which data can be transferred outside the EU. Transfers can only be allowed where these conditions, which safeguard the individuals' rights to a high level of protection, are met¹⁸.

Thirdly, concerning enforcement, the proposed rules provide for proportionate and dissuasive sanctions (up to 2% of a company's annual global turnover) to make sure that companies comply with EU law¹⁹. The existence of credible sanctions will increase companies' incentive to comply with EU law.

Fourthly, the proposed regulation includes clear rules on the obligations and liabilities of data processors such as cloud providers, including on security²⁰. As the revelations about US intelligence collection programmes have shown, this is critical because these programmes affect data stored in the cloud. Also, companies providing storage space in the cloud which are asked to provide personal data to foreign authorities will not be able to escape their responsibility by reference to their status as data processors rather than data controllers.

Fifth, the package will lead to the establishment of comprehensive rules for the protection of personal data processed in the law enforcement sector.

It is expected that the package will be agreed upon in a timely manner in the course of 2014²¹.

3.2. Making Safe Harbour safer

The Safe Harbour scheme is an important component of the EU-US commercial relationship, relied upon by companies on both sides of the Atlantic.

The Commission's report on the functioning of Safe Harbour has identified a number of weaknesses in the scheme. As a result of a lack of transparency and of enforcement, some self-certified Safe Harbour members do not, in practice, comply with its principles. This has a negative impact on EU citizens' fundamental rights. It also creates a disadvantage for European companies compared to those competing US companies that are operating under the scheme but in practice not applying its principles. This weakness also affects the majority of US companies which properly apply the scheme. Safe Harbour also acts as a conduit for the

with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

¹⁷ The Commission takes note that the European Parliament confirmed and strengthened this important principle, enshrined in Art. 3 of the proposed Regulation, in its vote of 21 October 2013 on the data protection reform reports of MEPs Jan-Philipp Albrecht and Dimitrios Droutsas in the Committee for Civil Liberties, Justice and Home Affairs (LIBE).

¹⁸ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee of the European Parliament proposed to include a provision in the future Regulation that would subject requests from foreign authorities to access personal data collected in the EU to the obtaining of a prior authorisation from a national data protection authority, where such a request would be issued outside a mutual legal assistance treaty or another international agreement.

¹⁹ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee proposed strengthening the Commission's proposal by providing that fines can go up to 5% of the annual worldwide turnover of a company.

²⁰ The Commission takes note that in its vote of 21 October 2013, the LIBE Committee endorsed the strengthening of the obligations and liabilities of data processors, in the particular with regard to Art. 26 of the proposed Regulation.

²¹ The Conclusions of the October 2013 European Council state that: "It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015".

transfer of the personal data of EU citizens from the EU to the US by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes. Unless the deficiencies are corrected, it therefore constitutes a competitive disadvantage for EU business and has a negative impact on the fundamental right to data protection of EU citizens.

The shortcomings of the Safe Harbour scheme have been underlined by the response of European Data Protection Authorities to the recent surveillance revelations. Article 3 of the Safe Harbour Decision authorises these authorities to suspend, under certain conditions, data flows to certified companies.²² German data protection commissioners have decided not to issue new permissions for data transfers to non-EU countries (for example for the use of certain cloud services). They will also examine whether data transfers on the basis of the Safe Harbour should be suspended.²³ The risk is that such measures, taken at national level, would create differences in coverage, which means that Safe Harbour would cease to be a core mechanism for the transfer of personal data between the EU and the US.

The Commission has the authority under Directive 95/46/EC to suspend or revoke the Safe Harbour decision if the scheme no longer provides an adequate level of protection. Furthermore, Article 3 of the Safe Harbour Decision provides that the Commission may reverse, suspend or limit the scope of the decision, while, under article 4, it may adapt the decision at any time in the light of experience with its implementation.

Against this background, a number of policy options can be considered, including:

- Maintaining the *status quo*;
- Strengthening the Safe Harbour scheme and reviewing its functioning thoroughly;
- Suspending or revoking the Safe Harbour decision.

Given the weaknesses identified, the current implementation of Safe Harbour cannot be maintained. However, its revocation would adversely affect the interests of member companies in the EU and in the US. The Commission considers that Safe Harbour should rather be strengthened.

The improvements should address both the structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception.

More specifically, for Safe Harbour to work as intended, the monitoring and supervision by US authorities of the compliance of certified companies with the Safe Harbour Privacy Principles needs to be more effective and systematic. The transparency of certified companies' privacy policies needs to be improved. The availability and affordability of dispute resolution mechanisms also needs to be ensured to EU citizens.

As a matter of urgency, the Commission will engage with the US authorities to discuss the shortcomings identified. Remedies should be identified by summer 2014 and implemented as soon as possible. On the basis thereof, the Commission will undertake a complete stock taking of the functioning of the Safe Harbour. This broader review process should involve open consultation and a debate in the European Parliament and the Council as well as discussions with the US authorities.

²² Specifically, pursuant to Art. 3 of the Safe Harbour Decision, such suspensions may take place in cases where there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

²³ Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, press release of 24 July 2013.

It is also important that the national security exception foreseen by the Safe Harbour Decision, is used only to an extent that is strictly necessary and proportionate.

3.3. Strengthening data protection safeguards in law enforcement cooperation

The EU and the US are currently negotiating a data protection “umbrella” agreement on transfers and processing of personal information in the context of police and judicial co-operation in criminal matters. The conclusion of such an agreement providing for a high level of protection of personal data would represent a major contribution to strengthening trust across the Atlantic. By advancing the protection of EU data citizens' rights, it would help strengthen transatlantic cooperation aimed at preventing and combating crime and terrorism.

According to the decision authorising the Commission to negotiate the umbrella agreement, the aim of the negotiations should be to ensure a high level of protection in line with the EU data protection *acquis*. This should be reflected in agreed rules and safeguards on, *inter alia*, purpose limitation, the conditions and the duration of the retention of data. In the context of the negotiation, the Commission should also obtain commitments on enforceable rights including judicial redress mechanisms for EU citizens not resident in the US²⁴. Close EU-US cooperation to address common security challenges should be mirrored by efforts to ensure that citizens benefit from the same rights when the same data is processed for the same purposes on both sides of the Atlantic. It is also important that derogations based on national security needs are narrowly defined. Safeguards and limitations should be agreed in this respect.

These negotiations provide an opportunity to clarify that personal data held by private companies and located in the EU will not be directly accessed by or transferred to US law enforcement authorities outside of formal channels of co-operation, such as Mutual Legal Assistance agreements or sectoral EU-US Agreements authorising such transfers. Access by other means should be excluded, unless it takes place in clearly defined, exceptional and judicially reviewable situations. The US should undertake commitments in that regard²⁵.

An “umbrella agreement” agreed along those lines, should provide the general framework to ensure a high level of protection of personal data when transferred to the US for the purpose of preventing or combating crime and terrorism. Sectoral agreements should, where necessary due to the nature of the data transfer concerned, lay down additional rules and safeguards, building on the example of the EU-US PNR and TFTP Agreements, which set strict conditions for transfer of data and safeguards for EU citizens.

²⁴ See the relevant passage of the Joint Press Statement following the EU-US-Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: “We are therefore, as a matter of urgency, committed to advancing rapidly in the negotiations on a meaningful and comprehensive data protection umbrella agreement in the field of law enforcement. The agreement would act as a basis to facilitate transfers of data in the context of police and judicial cooperation in criminal matters by ensuring a high level of personal data protection for U.S. and EU citizens. We are committed to working to resolve the remaining issues raised by both sides, including judicial redress (a critical issue for the EU). Our aim is to complete the negotiations on the agreement ahead of summer 2014.”

²⁵ See the relevant passage of the Joint Press Statement following the EU-US Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: “We also underline the value of the EU-U.S. Mutual Legal Assistance Agreement. We reiterate our commitment to ensure that it is used broadly and effectively for evidence purposes in criminal proceedings. There were also discussions on the need to clarify that personal data held by private entities in the territory of the other party will not be accessed by law enforcement agencies outside of legally authorized channels. We also agree to review the functioning of the Mutual Legal Assistance Agreement, as contemplated in the Agreement, and to consult each other whenever needed.”

3.4. Addressing European concerns in the on-going US reform process

US President Obama has announced a review of US national security authorities' activities, including of the applicable legal framework. This on-going process provides an important opportunity to address EU concerns raised by recent revelations about US intelligence collection programmes. The most important changes would be extending the safeguards available to US citizens and residents to EU citizens not resident in the US, increased transparency of intelligence activities, and further strengthening oversight. Such changes would restore trust in EU-US data exchanges, and promote the use of Internet services by Europeans.

With respect to extending the safeguards available to US citizens and residents to EU citizens, legal standards in relation to US surveillance programmes which treat US and EU citizens differently should be reviewed, including from the perspective of necessity and proportionality, keeping in mind the close transatlantic security partnership based on common values, rights and freedoms. This would reduce the extent to which Europeans are affected by US intelligence collection programmes.

More transparency is needed on the legal framework of US intelligence collection programmes and its interpretation by US Courts as well as on the quantitative dimension of US intelligence collection programmes. EU citizens would also benefit from such changes.

The oversight of US intelligence collection programmes would be improved by strengthening the role of the Foreign Intelligence Surveillance Court and by introducing remedies for individuals. These mechanisms could reduce the processing of personal data of Europeans that are not relevant for national security purposes.

3.5. Promoting privacy standards internationally

Issues raised by modern methods of data protection are not limited to data transfer between the EU and the US. A high level of protection of personal data should also be guaranteed to any individual. EU rules on collection, processing and transfer of data should be promoted internationally.

Recently, a number of initiatives have been proposed to promote the protection of privacy, particularly on the internet²⁶. The EU should ensure that such initiatives, if pursued, fully take into account the principles of protecting fundamental rights, freedom of expression, personal data and privacy as set out in EU law and in the EU Cyber Security Strategy, and do not undermine the freedom, openness and security of cyber space. This includes a democratic and efficient multi stakeholder governance model.

The on-going reforms of data protection laws on both sides of the Atlantic also provide the EU and the US a unique opportunity to set the standard internationally. Data exchanges across the Atlantic and beyond would greatly benefit from the strengthening of the US domestic legal framework, including the passage of the "Consumer Privacy Bill of Rights" announced by President Obama in February 2012 as part of a comprehensive blueprint to improve consumers' privacy protections. The existence of a set of strong and enforceable data protection rules enshrined in both the EU and the US would constitute a solid basis for cross-border data flows.

In view of promoting privacy standards internationally, accession to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), which is open to countries which are not member of the Council of Europe²⁷, should also be favoured. Safeguards and guarantees agreed in international fora should result in a high level of protection compatible with what is required under EU law.

²⁶ See in this respect the draft resolution proposed to the UN General Assembly by Germany and Brazil – calling for the protection of privacy online as offline.

²⁷ The US is already party to another Council of Europe convention: the 2001 Convention on Cybercrime (also known as the "Budapest Convention").

4. CONCLUSIONS AND RECOMMENDATIONS

The issues identified in this Communication require action to be taken by the US as well as by the EU and its Member States.

The concerns around transatlantic data exchanges are, first of all, a wake-up call for the EU and its Member States to advance swiftly and with ambition on the data protection reform. It shows that a strong legislative framework with clear rules that are enforceable also in situations when data are transferred abroad is, more than ever, a necessity. The EU institutions should therefore continue working towards the adoption of the EU data protection reform by spring 2014, to make sure that personal data is effectively and comprehensively protected.

Given the significance of transatlantic data flows, it is essential that the instruments on which these exchanges are based appropriately address the challenges and opportunities of the digital era and new technological developments like cloud computing. Existing and future arrangements and agreements should ensure that the continuity of a high level of protection is guaranteed over the Atlantic.

A robust Safe Harbour scheme is in the interests of EU and US citizens and companies. It should be strengthened by better monitoring and implementation in the short term, and, on this basis, by a broader review of its functioning. Improvements are necessary to ensure that the original objectives of the Safe Harbour Decision – i.e. continuity of data protection, legal certainty and free EU-US flow of data – are still met.

These improvements should focus on the need for the US authorities to better supervise and monitor the compliance of self-certified companies with the Safe Harbour Privacy Principles.

It is also important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary and proportionate.

In the area of law enforcement, the current negotiations of an “umbrella agreement” should result in a high level of protection for citizens on both sides of the Atlantic. Such an agreement would strengthen the trust of Europeans in EU-US data exchanges, and provide a basis to further develop EU-US security cooperation and partnership. In the context of the negotiation, commitments should be secured to the effect that procedural safeguards, including judicial redress, are available to Europeans who are not resident in the US.

Commitments should be sought from the US administration to ensure that personal data held by private entities in the EU will not be accessed directly by US law enforcement agencies outside of formal channels of co-operation, such as Mutual Legal Assistance agreements and sectoral EU-US Agreements such as PNR and TFTP authorising such transfers under strict conditions, except in clearly defined, exceptional and judicially reviewable situations.

The US should also extend the safeguards available to US citizens and residents to EU citizens not resident in the US, ensure the necessity and proportionality of the programmes, greater transparency and oversight in the legal framework applicable to US national security authorities.

Areas listed in this communication will require constructive engagement from both sides of the Atlantic. Together, as strategic partners, the EU and the US have the ability to overcome the current tensions in the transatlantic relationship and rebuild trust in EU-US data flows. Undertaking joint political and legal commitments on further cooperation in these areas will strengthen the overall transatlantic relationship.